Reversible BCH符号と合成体を使った有限体の計算

情報数理学特別講義I 第12回

2025-11-07

巡回符号の最小距離

定理 8.2
$GF(p)$ 上の長さ $n = p^q - 1$ の巡回符号 $\mathcal{C}$ を考えよう．$\mathcal{C}$ の生成多項式を $g(x), \beta \in GF(p^q)$ を位数 n の元とし，ある非負の整数 a が存在して，$d-1$ 個の連続した指数を持つ $\beta^a, \beta^{a+1}, \ldots, \beta^{a+d-2}$ が $g(x)$ の根であるとする．このとき，巡回符号 $\mathcal{C}$ の最小距離 $d_{\min}(\mathcal{C})$ について $d_{\min}(\mathcal{C}) \geq d$ が成り立つ.

t 誤り訂正のBCH符号の場合,

β^a を原始元 α とすると，$g(x)$ が $\alpha, \alpha^2, \ldots, \alpha^{2t}$ の指数が連続した根を持つ．この時BCH符号の最小距離は $2t+1$ 以上となる.

クイズ：4つの誤りを訂正するBCH符号の場合，何個連続した根を持てば良い？

2元BCH符号の最小距離

訂正数 t に対して，最小距離は $2t+1$ 以上つまり奇数となる.

最小距離が偶数となる2元BCH符号は作れないのか？

最小距離が偶数となる2元BCH符号は作れる.

単一パリティ検査符号のように全ビットの総和１ビットのパリティを付加すればよい.
$(x+1)$ を生成多項式に含む巡回符号の最小距離は偶数になる.
2元BCH符号であれば，生成多項式 $g(x)$ に $x+1$ をかけた生成多項式 $g'(x)=(x+1)g(x)$ で符号化すればい.

生成多項式 $g(x)$ で定義されるt誤り訂正可能な2元BCH符号 $\mathcal{C}$ の最小距離が $2t+1$ のとき，生成多項式 $g'(x)=(x+1)g(x)$ で構成される2元BCH符号$\mathcal{C}'$ の最小距離は $2t+2$.

質問：最小距離を１増やすメリットは？

根は必ずしも $\alpha, \ldots, \alpha^{2t}$ でなくてもよい.

例えば, $g(x) = (x+1)\mu_{\alpha}(x)\mu_{\alpha^3}(x)$ で構成されたBCH符号 $\mathcal{C}$ と,
$g'(x) = (x+1)\mu_{\alpha}(x)\mu_{\alpha^{-1}}(x)$ で構成されたBCH符号 $\mathcal{C}'$ の最小距離は共に 6 となる.

Reversible Code

$g'(x) = \mu_{\alpha^{-t}}(x) \cdots (x+1) \cdots \mu_{\alpha^{t}}(x)$ で構成されたBCH符号は Reversible BCH符号と呼ばれ,
符号ビットを逆順にした系列も符号語となるという特徴を持つ.

つまり

$$\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$$

ならば

$$\underline{c}' = (c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathcal{C}$$

となる.

練習問題1：2誤り訂正 Reversible BCH符号

ただし，α は原始多項式 $p(x) = 1 + x + x^4$ の根とし，長さ 15 の符号とする.
(1) 生成多項式 $g(x) = \mu_{\alpha^{-1}}(x)(x+1)\mu_{\alpha}(x)$ で構成されるBCH符号の生成多項式を計算し（和形式に展開するということ），その生成多項式の特徴を述べよ.
(2) 逆順にした系列も符号語となることを確認せよ.

Reversible BCH符号の誤り位置多項式の計算

通常の2誤り訂正BCH符号では，生成多項式がαとα^3を根に持つため，シンドローム$S_1 = r(\alpha)$と$S_3 = r(\alpha^3)$を用い，$(S_1^3 - S_3)S_1^{-1}$を計算して誤り位置多項式$\sigma(x)$の定数項を得た．この立式には3乗計算と複数回の乗算が含まれていた．

一方，Reversible BCH符号では$g'(x) = (x+1)\mu_{\alpha^{-1}}(x)\mu_{\alpha}(x)$のように相反な根を必ず対で含むため，$\alpha$だけでなく$\alpha^{-1}$に対するシンドローム$S_{-1} = r(\alpha^{-1})$が自動的に得られる．受信語$r(x)$に対して$i+1$ビット目と$j+1$ビット目に誤りがあるとき

- $S_1 = \alpha^i + \alpha^j$,
- $S_{-1} = \alpha^{-i} + \alpha^{-j} = \alpha^{-(i+j)}\left(\alpha^i + \alpha^j\right) = \alpha^{-(i+j)}S_1$
  が成り立つ．よって$\alpha^{i+j} = S_1 S_{-1}^{-1}$が直接求められ，誤り位置多項式

$$\sigma(x) = (x+\alpha^i)(x+\alpha^j) = S_1 S_{-1}^{-1} - S_1 x + x^2$$

が2つのシンドロームだけで記述できる．必要な操作はS_{-1}の逆元計算と1回の乗算のみであり，で示した通常の2誤り訂正BCH符号よりも計算複雑度が低い．

合成体を使った有限体の計算

$GF(2^q)$上の逆元計算や$\log_\alpha$演算をテーブル参照により回路実装した場合，テーブルの要素の数が2^q個となるため，回路規模が非常に大きくなるという問題がある．
この問題を解決する一つの方法として，$GF(2^q)$の同型写像である合成体$GF((2^{q_s})^{q_c})$を用いる方法がある．

例えば $GF(2^q)$ 上のある元 a の逆元 a^{-1} を求める際，まず合成体$GF((2^{q_s})^{q_c})$上の元 c へ写像し，c の逆元 c^{-1} を計算する，そしてその c^{-1} を $GF(2^q)$ 上へ逆写像することで，所望の逆元 a^{-1} を得る．

部分体$GF(2^{q_s})$の構成

まず部分体 $GF(2^{q_s})$ を構成するため，最大次数が q_s の $GF(2)$ 上の既約多項式 $p_s(x)$ を求める．この既約多項式 $p_s(x)$ は，位数が $2^{q_s}-1$ の元 $\beta \in GF(2^q)$ の最小多項式 $m_\beta(x)$ とすればよいので，$\beta = \alpha^l, l = \dfrac{2^q-1}{2^{q_s}-1}$ とし，この元 β の共役な元を全て根に持つ多項式

$$p_s(x) = (\beta + x)(\beta^2 + x)\cdots(\beta^{2^{q_s-1}} + x)$$

によって$GF(2^{q_s})$を構成する．

例：$GF(2^4)$ の同型写像である合成体$GF((2^2)^2)$を構成する際の部分体$GF(2^2)$を考えてみよう．$GF(2^4)$の中で部分体$GF(2^2)$を構成する元βは，$\dfrac{2^4-1}{2^2-1} = 5$より，

$\beta = \alpha^5$．よって既約多項式 $p_s(x)$ は

$$p_s(x) = (\alpha^5 + x)(\alpha^{10} + x) = 1 + x + x^2.$$

部分体$GF(2^2)$の対応関係

べき表現	$GF(2^4)$の元によるべき表現	$GF(2^4)$の元による多項式表現	ベクトル表現
0	0	0	$(0,0)$
1	1	1	$(1,0)$
β	α^5	α^5	$(0,1)$
β^2	α^{10}	$1+\alpha^5$	$(1,1)$

ただし β を $p_s(x)=1+x+x^2$ の根とする.

練習問題2： 部分体$GF(2^2)$が加算と乗算について群をなすことを確かめよう.
ヒント：加算と乗算について演算表を作成すれば良い

部分体$GF(2^{q_s})$の拡大による合成体$GF((2^{q_s})^{q_c})$の構成

前節で構成した部分体$GF(2^{q_s})$を合成体$GF((2^{q_s})^{q_c})$へ拡大するための最大次数がq_cの$GF(2^{q_s})$上の既約多項式$p_c(x)$を次のように定義する.

$$p_c(x) = (\alpha + x)(\alpha^{2^{q_s}} + x) \cdots (\alpha^{(2^{q_s})^{q_c-1}} + x)$$

$p_c(x)$は$\alpha \in GF(2^q)$を根に持ち，さらに係数が$GF(2^{q_s})$上の元となる$GF(2^{q_s})$上の既約多項式である.

これにより，合成体$GF((2^{q_s})^{q_c})$の元cは，次のような多項式で表現できる.

$$c(\alpha) = c_0 + c_1\alpha + \cdots + c_{q_c-1}\alpha^{q_c-1},$$

ただし $c_i \in GF(2^{q_s}), i \in \{0, 1, \ldots, q_c - 1\}$.

ベクトル表現の際には 上式の各係数を並べ $c = (c_0, c_1, \ldots, c_{q_c-1})^{\mathrm{T}}$ とすれば良い．各c_iはq_sビットの2元ベクトル$(c_{i0}, c_{i1}, \ldots, c_{i(q_s-1)})^T$で表現され，それが$q_c$個あるため，合成体の元も，もとのガロア体の元と同様$q_s q_c = q$ビットで表現される.

$GF(2^2)$ を 合成体$GF((2^2)^2)$ に拡大する多項式$p_c(x)$

先に定義した部分体$GF(2^2)$を$GF((2^2)^2)$へ拡大するための既約多項式$p_c(x)$を次のように定義する.

$$p_c(x) = (\alpha + x)(\alpha^4 + x) = \alpha^5 + x + x^2$$

上式を見るとわかるように，多項式の係数は全て部分体$\{0, 1, \alpha^5, \alpha^{10}\}$の元となっている.
$p_c(x)$の根 α を使って，$GF((2^2)^2)$上の元 c' は

$$c' = c'_0 + c'_1\alpha$$

とかける．ただし $c'_0, c'_1 \in GF(2^2)$.
以上より，合成体$GF((2^2)^2)$が定義できた.

合成体$GF((2^2)^2)$からガロア体$GF(2^4)$への写像

合成体$GF((2^2)^2)$の元c'のベクトル表現$\underline{c'}$からガロア体$GF(2^4)$の元a'のベクトル表現$\underline{a'}$への写像を考えてみよう．$c'_i \in GF(2^2), i \in \{0,1\}$ は $c'_i = c'_{i0} + c'_{i1}\alpha^5$, ただし $c'_{i0}, c'_{i1} \in GF(2)$, で表現できることから

$$
\begin{aligned}
c' &= c'_0 + c'_1\alpha \\
&= c'_{00} + c'_{01}\alpha^5 + (c'_{10} + c'_{11}\alpha^5)\alpha \\
&= (1, \alpha^5, \alpha, \alpha^6) \begin{pmatrix} c'_{00} \\ c'_{01} \\ c'_{10} \\ c'_{11} \end{pmatrix}.
\end{aligned}
$$

$\underline{c'} = (c'_{00}, c'_{01}, c'_{10}, c'_{11})^{\mathrm{T}}$ は$GF((2^2)^2)$の元c'のベクトル表現なので，$(1, \alpha^5, \alpha, \alpha^6)$ が合成体$GF((2^2)^2)$からガロア体$GF(2^4)$への写像 T' となり，その2元行列表現は

$$T' = (1, \alpha^5, \alpha, \alpha^6) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

として与えらえる．そしてその逆行列

$$T'^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

がガロア体$GF(2^4)$から合成体$GF((2^2)^2)$への写像 T となる．

Table 1: Elements in Galois field $GF(2^4)$ and its composite field $GF((2^2)^2)$.

Elements in $GF(2^4)$		Elements in $GF((2^2)^2)$	
Power repr.	Vector repr. a_0, a_1, a_2, a_3	Polynomial repr. $c'_0 + c'_1\alpha$	Vector repr. $c'_{00}, c'_{01}, c'_{10}, c'_{11}$
0	$0,0,0,0$	0	$0,0,0,0$
1	$1,0,0,0$	1	$1,0,0,0$
α	$0,1,0,0$	α	$0,0,1,0$
α^2	$0,0,1,0$	$\beta + \alpha$	$0,1,1,0$
α^3	$0,0,0,1$	$\beta + \beta^2\alpha$	$0,1,1,1$
α^4	$1,1,0,0$	$1 + \alpha$	$1,0,1,0$
α^5	$0,1,1,0$	β	$0,1,0,0$
α^6	$0,0,1,1$	$\beta\alpha$	$0,0,0,1$
α^7	$1,1,0,1$	$\beta^2 + \beta\alpha$	$1,1,0,1$
α^8	$1,0,1,0$	$\beta^2 + \alpha$	$1,1,1,0$
α^9	$0,1,0,1$	$\beta + \beta\alpha$	$0,1,0,1$
α^{10}	$1,1,1,0$	β^2	$1,1,0,0$
α^{11}	$0,1,1,1$	$\beta^2\alpha$	$0,0,1,1$
α^{12}	$1,1,1,1$	$1 + \beta^2\alpha$	$1,0,1,1$
α^{13}	$1,0,1,1$	$1 + \beta\alpha$	$1,0,0,1$
α^{14}	$1,0,0,1$	$\beta^2 + \beta^2\alpha$	$1,1,1,1$

$GF((2^{q_s})^{q_c})$上の逆元計算

合成体 $GF((2^{q_s})^{q_c})$ 上で逆元を計算するアルゴリズムのうち，部分体 $GF(2^{q_s})$ への射影を利用した逆元計算を紹介する．別の方法としてユークリッドアルゴリズムを使う方法もある．

部分体$GF(2^{q_s})$への射影を利用した逆元計算

元$c \in GF((2^{q_s})^{q_c})$の$l = \dfrac{2^{q_s q_c} - 1}{2^{q_s} - 1}$乗が部分体$GF(2^{q_s})$の元になることを利用して逆元$c^{-1}$を計算する．計算は以下の4ステップとなる．

1. c^{l-1}を計算する．
2. $c^l = c^{l-1} \cdot c$を計算する．
3. $(c^l)^{-1}$を計算する．c^lは$GF(2^{q_s})$の元なので逆元は2^{q_s}個の要素のテーブルで計算可能
4. $c^{-1} = (c^l)^{-1} \cdot (c^{l-1})$を計算する．

ポイントは 2. で計算されるc^lが部分体$GF(2^{q_s})$の元，つまり長さq_sの2元ベクトル表現に縮退されるところで，これにより 3. の逆元演算に必要なテーブルの要素数が2^{q_s}個となり，ガロア体の逆元テーブルの要素数 $2^{q_s q_c}$ と比べて要素数は$\dfrac{2^{q_s}}{2^{q_s q_c}} = \dfrac{1}{2^{q_s(q_c-1)}}$となり，要素数を大きく削減することができる．

練習問題3：合成体$GF((2^2)^2)$の元$\beta + \alpha$の逆元計算

上述した4ステップで$c' = \beta + \alpha \in GF((2^2)^2)$の逆元を計算しよう.

1. c^{l-1}を計算する.
2. $c^l = c^{l-1} \cdot c$を計算する.
3. $(c^l)^{-1}$を計算する.
4. $c^{-1} = (c^l)^{-1} \cdot (c^{l-1})$を計算する.